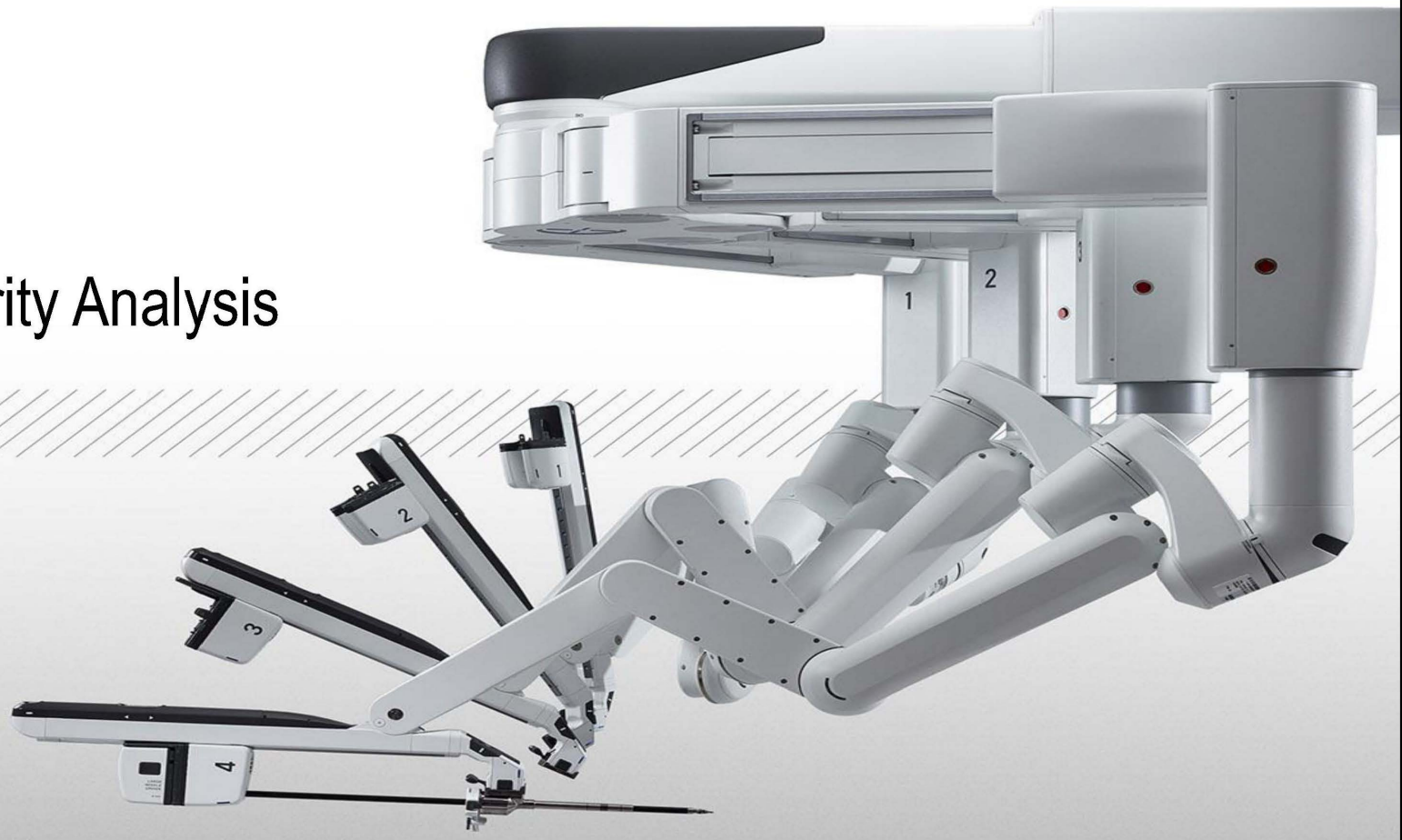
INTUITIVE SURGICAL®

Instrument Security Analysis

November 2019

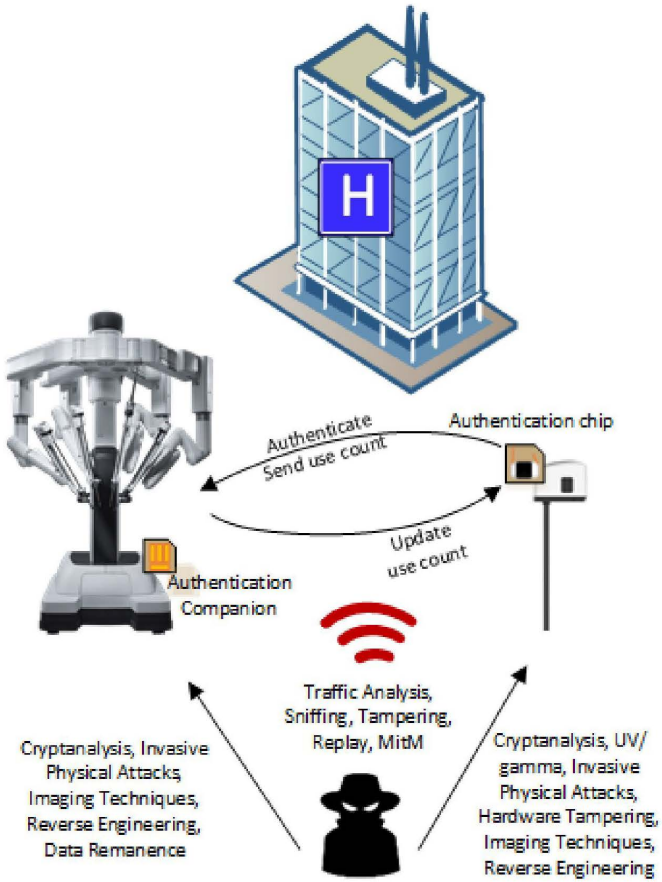


da Vinci Surgery

Overview

- Concerns
  - Counterfeit instruments
  - Tampering with the use count values / reprocessing
- Security requirements
  - Authentication to recognize and accept only ISI instruments
  - Secure storage, retrieval, and update of the use count values
  - Must function even when the system is offline
- Technology

Product	Authentication chip	Interface	Counterfeit Auth Key	Use count	Security Level
Si	Dallas DS2505 (Production year ~1995)	1-wire	Passcode	OTP	Low
X/Xi/SP	Atmel AT88SC6416CRF (Production year ~2004)	RF	Secret Key	OTP	Medium
Orion2	Atmel AT88SC6416CRF (Production year ~2004)	RF	Secret Key	OTP	Medium / High
Ion	Maxim Secure Authenticator - DS28E36 (Production year 2017)	1-wire	PKI / ECC	OTP	High



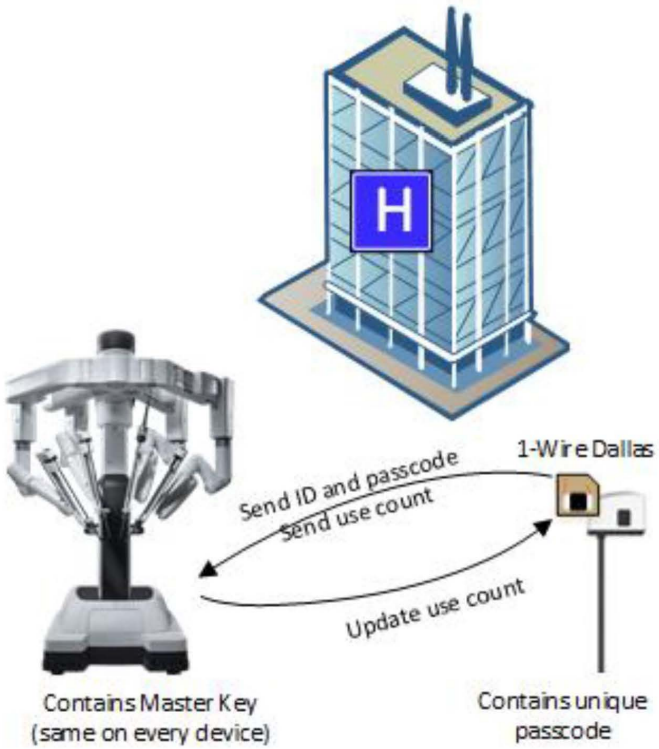
Si Instruments

- Authentication scheme
  - System has a Master Key (same key in every da Vinci)
  - Each instrument (Dallas DS2505) is programmed with a unique passcode derived from Master Key and instrument ID
  - During authentication, instrument sends its ID and the passcode to the system
  - System verifies the passcode by computing the expected value from the instrument ID and the Master Key
- Weaknesses
  - Communication channel is not encrypted. Scheme is susceptible to Replay and Man-in-the-Middle

    -> Capture a pair of (ID, passcode) and replay it on counterfeits

    -> Tamper with the traffic to send fake use counts
  - Master Key is hardcoded and is not well protected in the system

    -> Disclosure of Master Key (e.g., reverse engineering, data remanence, internal employees) allows one to easily program vanilla D2505 with right passcodes
  - Key /passcode length is short and brute-force is possible
  - Physical attacks to chips (e.g., UV, gamma) are possible



X/Xi/SP Instruments

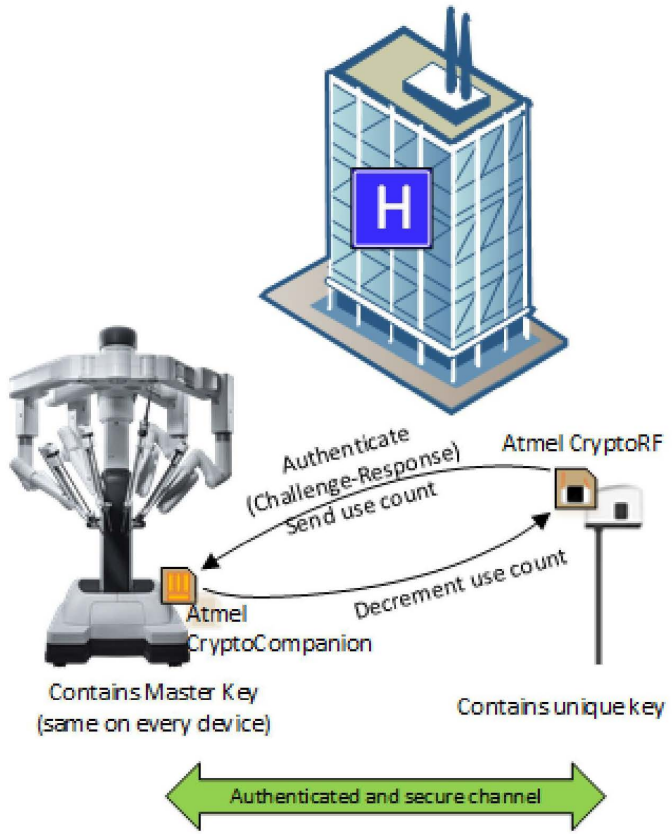
- Authentication scheme
  - System has a Master Key (same key in every da Vinci) stored in CryptoCompanion
  - Each instrument (CryptoRF) is programmed with a unique key derived from Master Key and its instrument ID
  - During authentication, system sends a challenge (random number) and CryptoRF computes a response using its unique key
  - System receives the response and invokes CryptoCompanion to verify it using the instrument ID and the challenge.
  - The keys never leave CryptoCompanion or CryptoRF
- Weaknesses
  - Master Key is protected by CryptoCompanion, but *may* still be susceptible to invasive Physical attacks (microprobing, imaging)

    -> Disclosure of Master Key allows one to derive the CryptoRF keys

    -> Atmel reserved a certain ID range for ISI. This provides some assurance, but one could use custom hardware to emulate CryptoRF and use a valid ID within that range
  - UV/gamma attacks to reset use-count, but we use decrement-only
  - There are published Cryptanalysis and side-channel attacks

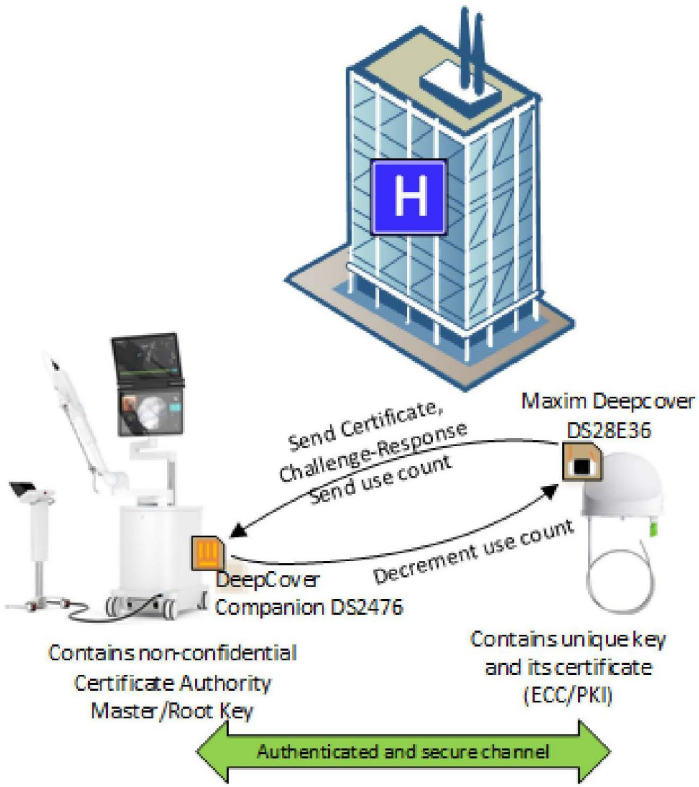
    -> Reveals only CryptoRF key. Still need to emulate a Tag to use the right ID
  - Communication channel is encrypted, but *may* still be susceptible to Replay and Man-in-the-Middle

    -> Encryption key used for use count and the rest of Cal data is the same. Copy-over from Cal data region.



Ion Instruments

- Authentication scheme
  - Completely relies on Public Key Cryptography (Elliptic Curve -ECC) with NIST recommended parameters and auth protocol
  - Maxim SecureAuthenticator chips are capable of generating their own keys and perform computations all inside the chip
  - Master key (Certificate Authority) is h/w protected and used only in manufacturing facility
  - During manufacturing, each instrument (SecureAuthenticator) generates a unique ECC key, goes through key verification and testing, and gets an ECC certificate for its key
  - Master key is only used to generate/sign the certificate. System trusts the Master key and thus the certificates signed by it
  - During authentication, the instrument presents its certificate to the system and performs a challenge-response protocol to prove its key
- Weaknesses
  - No weaknesses known
- Strengths
  - Keys are never exposed.
  - Use count is stored in decrement-only OTP
  - SecureAuthenticator employs built-in mitigations against several common attacks



Orion2 Instruments

- Authentication scheme
  - Minimum Viable Product: Same as Gen4
  - Proposed (Optional) Mitigations:
    - Hardware mitigation: Use a more advanced authenticator chip (such as 1-Wire DS28E36 in Ion) in addition to Atmel CrytoRF (Gen4)
      - Provides better security compared to what is used in Gen4
      - Dual protection is recommended given the expected product life of 15+ years
      - Impact on the cost basis. DS28E36 is around $2 in bulk. WCM (which also includes Flash memory) is $38.
    - Software mitigations (under investigation/design):
      - Different encryption keys for use count value and cal data
        - May break Gen4 compatibility
      - Use a tool database to blacklist compromised and/or consumed instrument IDs
        - Requires discussions and design of the processes to compile and distribute the data
      - Better protection for the secrets in the system
- Weaknesses
  - MVP: Same as Gen4
  - With additional mitigations: Still vulnerable to key disclosure unless we use a more advanced authenticator
    - Physical attacks on CryptoCcompanion (System) to disclose the Master Key